Big Brother als baas

Koops, E.J.

Published in:
Informatie : Maandblad voor de Informatievoorziening

Publication date:
2000

Koops, B.J. (2000). Big Brother als baas. verschenen in *Informatie : Maandblad voor de Informatievoorziening, 42*(september), 42-43

Big Brother als baas

Laatst kreeg ik een zorgelijk telefoontje van een vriend van me die werkt bij een webwinkel. Hij had een netbericht gestuurd naar een collega binnen het bedrijf, waarin hij vertelde dat hij sollicitatieplannen had – zijn baas begon hem een beetje de keel uit te hangen. Hij wist dat zijn collega die dag niet aanwezig was, maar kreeg toch even later een automatisch antwoord dat het bericht was gelezen. Lichte paniek – zou de werkgever het netwerkverkeer automatisch controleren? Of misschien zelfs filteren op trefwoorden als "sollicitatie"? Het is bepaald niet ondenkbeeldig – volgens een recente studie controleert 45% van alle bedrijven in de VS op een of andere manier het telefoon-, e-post- en Internetverkeer van de werknemers. Zou dat in Nederland ook zomaar mogen?

Sommige mensen (vooral werkgevers) vinden dat alles binnen bedrijf een zakelijk karakter heeft: op de werkvloer bestaat geen privé-sfeer. Een dergelijke opvatting is echter niet meer van deze tijd. Onze drukke en flexibele netwerkmaatschappij functioneert alleen maar als werknemers ook onder werktijd privé-aangelegenheden kunnen regelen – het spreekwoordelijke telefoontje dat er wordt overgewerkt, snel op het Internet opzoeken hoe laat de film vanavond begint, of even op de webcam thuis kijken of de kinderoppas de kinderen niet mishandelt.

Daar komt nog bij dat met de introductie van e-post ook de communicatiestijl van werknemers is veranderd. Een berichtje is informeler en directer dan een brief of memo, en minder hoorbaar voor collega's op zaal dan de telefoon. Het gevolg is dat men in e-berichten vaker dan vroeger opmerkingen maakt die in de privé-sfeer thuishoren.

Daarom kunnen werkgevers niet zomaar al het netverkeer aftappen. Dat wil ook weer niet zeggen dat ze het nooit zouden mogen. Want de informele e-cultuur heeft ook geleerd dat werknemers nogal wat werktijd op het Internet doorbrengen, inclusief de blote gedeelten daarvan, terwijl bedrijfsnetwerken soms aanzienlijk worden vertraagd door een niet altijd even zakelijk samenzijn van collega's in netwerkspelletjes. En sommige werknemers blijken e-post ook te misbruiken met schadelijker gevolgen, zoals seksuele intidimatie, racistische uitlatingen of het weglekken van bedrijfsgeheimen. Werkgevers kunnen dus zeker een legitiem belang hebben om het netwerkgebruik te controleren.

De baas zal daarom de middenweg moeten bewandelen van een effectieve controle op misstanden in het netwerk die de privacy van werknemers niet te veel schaadt. De hamvraag is natuurlijk: waar loopt die middenweg?

Wet en rechtspraak bieden algemene normen waar controlerende bazen zich aan moeten houden. Allereerst biedt het strafrecht enig houvast: de afluisterbepalingen (art. 139a-c Wetboek van Strafrecht) kennen uitzonderingen voor werkgevers: zij kunnen straffeloos telecomverkeer van werknemers opnemen, "behoudens in geval van kennelijk misbruik". De controlemogelijkheid wordt verder ingeperkt door het burgerlijk recht, waarin de

norm van het "goed werkgeverschap" (art. 7:611 Burgerlijk Wetboek) in rechtspraak nader is uitgewerkt. De belangrijkste en meest concrete bepalingen zijn te vinden in de Wet Bescherming Persoonsgegevens (WBP, de opvolger van de Wet persoonsregistraties die begin 2001 in werking treedt) en in de Wet op de ondernemingsraden.

Uit al deze normen en regels kan men richtlijnen destilleren voor bedrijven die werknemers willen controleren. Daarbij kan men ook gebruikmaken van bijvoorbeeld de vuistregels van de Registratiekamer en het voorbeeldprotocol van FNV Bondgenoten over privacy bij Internet- en e-postgebruik. De volgende richtlijnen zijn van belang.

1. Terughoudendheid

Het uitgangspunt bij controle is terughoudendheid. De werkgever mag in principe wel afluisteren, registreren of observeren, maar alleen met de minst ingrijpende middelen ("subsidiariteit") en alleen voorzover nodig om het doel te bereiken ("proportionaliteit"). Zo is een steekproefcontrole bij bepaalde afdelingen minder ingrijpend dan routinecontrole van al het netverkeer. Ook past terughoudendheid in de keuze van controlemethoden. Zo is er bij camera-observatie al snel sprake van het vastleggen van "gevoelige gegevens" (zoals ras of medische kenmerken) die extra bescherming genieten op grond van de WBP; het is daarom alleen toelaatbaar als er echt geen andere mogelijkheden zijn om het doel te bereiken.

2. Noodzakelijk belang en doelbinding

Verder moet controle van netwerkverkeer noodzakelijk zijn voor de behartiging van een gerechtvaardigd belang van de werkgever. Zo'n belang kan bijvoorbeeld zijn:

- *kostenbeheersing*, bijvoorbeeld om dure telefoontjes naar mobiele of exotische bestemmingen in de hand te houden. Vanwege het principe van terughoudendheid moet de controle zo beperkt mogelijk zijn, bijvoorbeeld alleen routinematig de totale telefoonkosten per eenheid vastleggen, en pas specifieker verkeersgegevens controleren als er ongebruikelijke pieken in de kosten opdoemen;
- *prestatiebeoordeling*: vooral belbureaus hebben belang bij het meten van de telefonische prestaties van werknemers, terwijl bedrijven zich ook zorgen kunnen maken over de kwaliteit van een elektronische hulpdienst. Maar daarvoor is het meestal niet nodig om de telecommunicatie op te nemen – het inschakelen van een bureau dat de dienstverlening test door "mystery customers" op de werknemers af te sturen is minder ingrijpend en net zo effectief;
- *opsporing van onrechtmatigheden*: zodra een bedrijf met reden vermoedt dat een (al dan niet bekende) werknemer zich elektronisch misdraagt, kan controle van het netwerkgebruik nodig zijn. Die controle moet dan wel zo specifiek mogelijk op de vermoedelijke misdrager(s) gericht zijn. Preventieve controle om het bedrijfsbeleid voor netwerkgebruik te handhaven is wel toegestaan, maar dit mag geen "Big Brother"-vormen aannemen – steekproeven op vooraf aangekondigde wijzen moeten volstaan.

Hierbij geldt steeds het principe van doelbinding: de gegevens die de controle oplevert mogen alleen worden gebruikt voor het specifieke doel van die controle.

3. Kenbaarheid

Een belangrijk criterium voor de geoorloofdheid van netwerkcontroles is de kenbaarheid daarvan voor de werknemers. Dat heeft deels te maken met "privacy-verwachting": een werknemer kan zich nu eenmaal minder snel beroepen op schending van de privacy als hij weet dat de baas alle netwerkverkeer filtert op "sex" en "sollicitatie", maar des te eerder als de baas zonder zijn medeweten meeluistert met de telefoon. Deels heeft het ook te maken met de rechten van werknemers (zie onder 4) – die kunnen ze immers alleen uitoefenen als ze überhaupt *weten* dat ze gecontroleerd kunnen worden. Daarom moeten werkgevers hun netwerkgebruikbeleid en de controle daarop kenbaar maken, bijvoorbeeld in het openingsscherm op de computer, maar ook in folders voor nieuwe werknemers of in het personeelsblaadje.

4. Rechten van betrokkenen

Omdat controle van netwerkgebruik al snel de privacy schendt, moet de baas de privacy-rechten van werknemers respecteren. In de WBP is bijvoorbeeld vastgelegd dat degenen van wie persoonsgegevens worden verwerkt het recht hebben op inzage in de registratie, op correctie als ze foute gegevens aantreffen, en op verwijdering als de gegevens niet langer relevant zijn.

5. Toestemming van de ondernemingsraad

Artikel 27 lid 1 onder 1 van de Wet op de ondernemingsraden bepaalt dat de ondernemingsraad toestemming moet geven voor het gebruik van "personeelsvolgsystemen". Vrijwel alle vormen van controle van netwerkgebruik vallen onder dit begrip, zodat de werkgever zijn controleplannen eerst moet voorleggen aan de ondernemingsraad. Dat komt natuurlijk ook de kenbaarheid ten goede.

De toepassing van deze richtlijnen zal per instantie verschillen. Zo moeten financiële instellingen aan strenge eisen voldoen, waardoor zij een groot belang hebben bij controle van het functioneren van werknemers. Maar mijn universiteit zal nauwelijks mijn netwerkgebruik kunnen reguleren (en dus ook niet controleren) – als academisch onderzoeker naar Internetcriminaliteit is het immers mijn werk om de duistere krochten van het Internet af te struinen, en om cd's te bestellen om privacypraktijken van webwinkels te kunnen beoordelen.

Met mijn webwinkelvriend is het overigens goed afgelopen. De systeembeheerder bleek net bij zijn collega een nieuw e-postprogramma te hebben geïnstalleerd en zijn berichtje – zonder te lezen – te hebben geopend. Inmiddels werkt hij bij een nieuwe baas – en heeft-i een folder over diens netwerkcontrolebeleid.

Bronnen

- 'Controle e-mail en internetgebruik op de werkplek', in *Privacy & Informatie* 1999/5, p. 237; in september publiceert de Registratiekamer een uitgebreider onderzoek hierover, zie <http://www.registratiekamer.nl>
- FNV Bondgenoten, *Voorbeeldprotocol: privacy bij internet- en email-gebruik*, <http://www.bondgenoten.fnv.nl/start/fbg/site-mz/vb-prtcl.htm>
- American Management Association, *Workplace Monitoring & Surveillance. 1999 AMA Survey*, <www.amanet.org/research/monit/index.htm>

Dr. Bert-Jaap Koops is senior-onderzoeker bij het Centrum voor Recht, Bestuur en Informatisering van de Katholieke Universiteit Brabant.